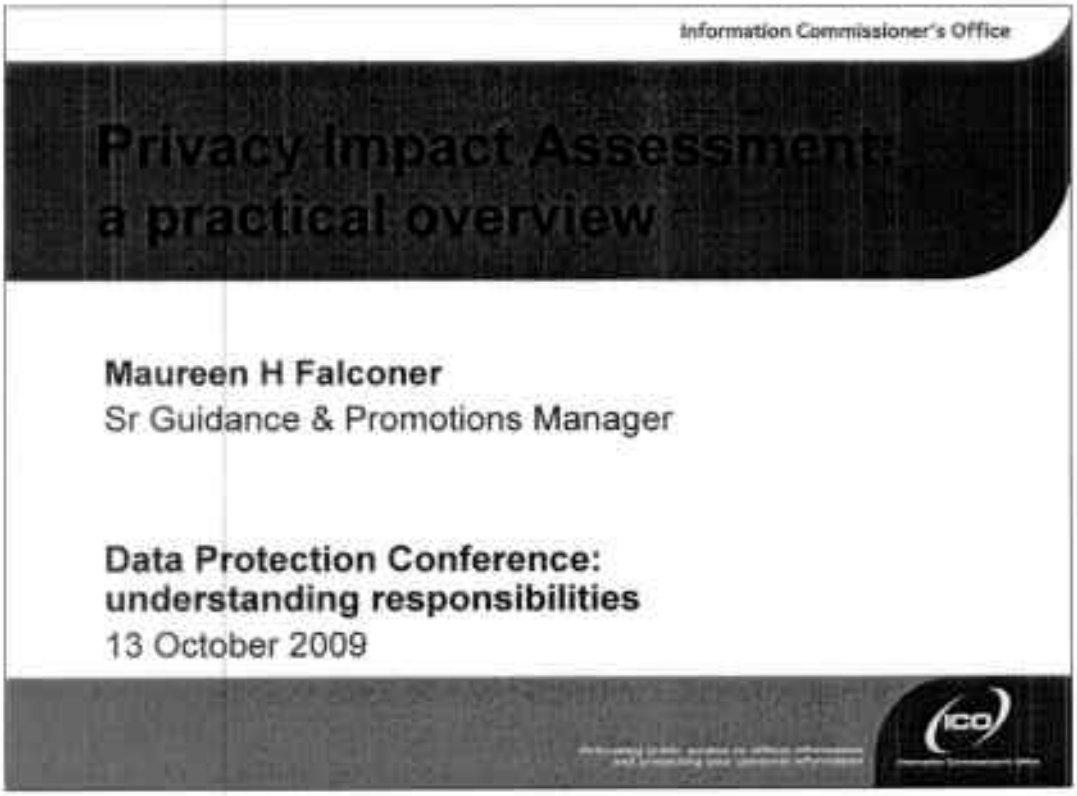
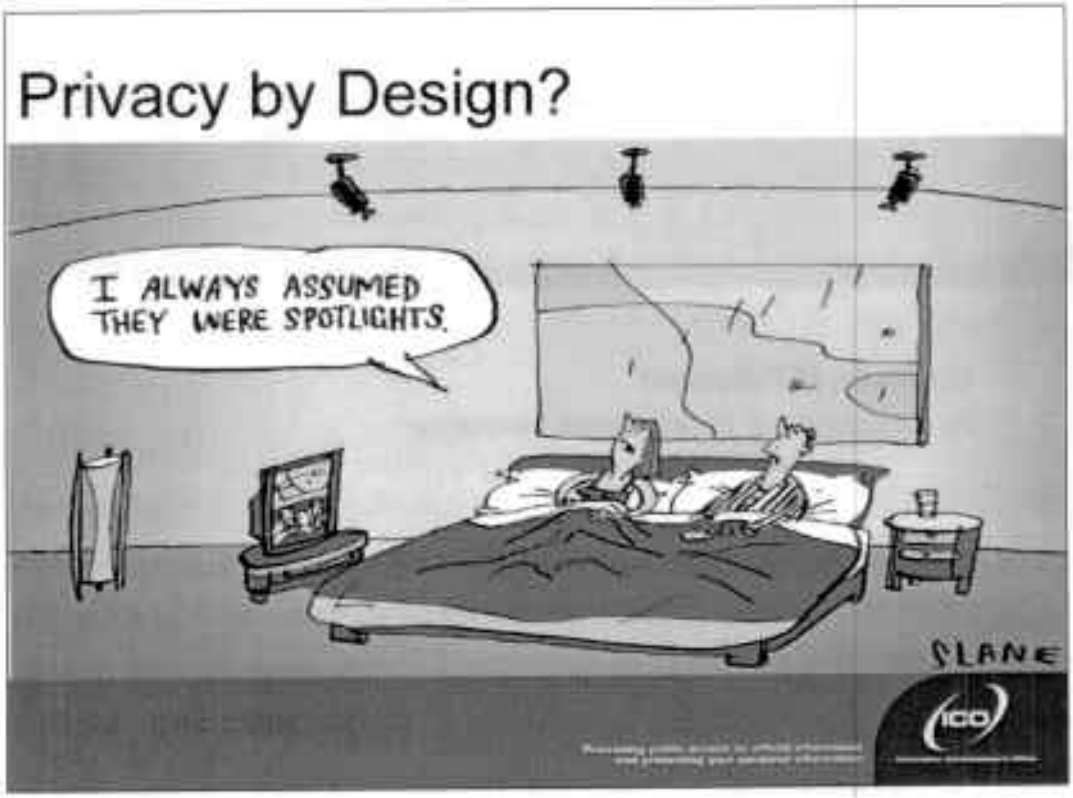

Information Commissioner's Office
Privacy Impact Assessment: a practical overview
Maureen H Falconer
Sr Guidance & Promotions Manager
Data Protection Conference: understanding responsibilities
13 October 2009



Increase in technology not commensurate with pace of privacy-friendly systems & processes. Sometimes this is due an inherent, antiquated system design but sometimes it's due to an emphasis on other risk factors at the expense of personal privacy!!

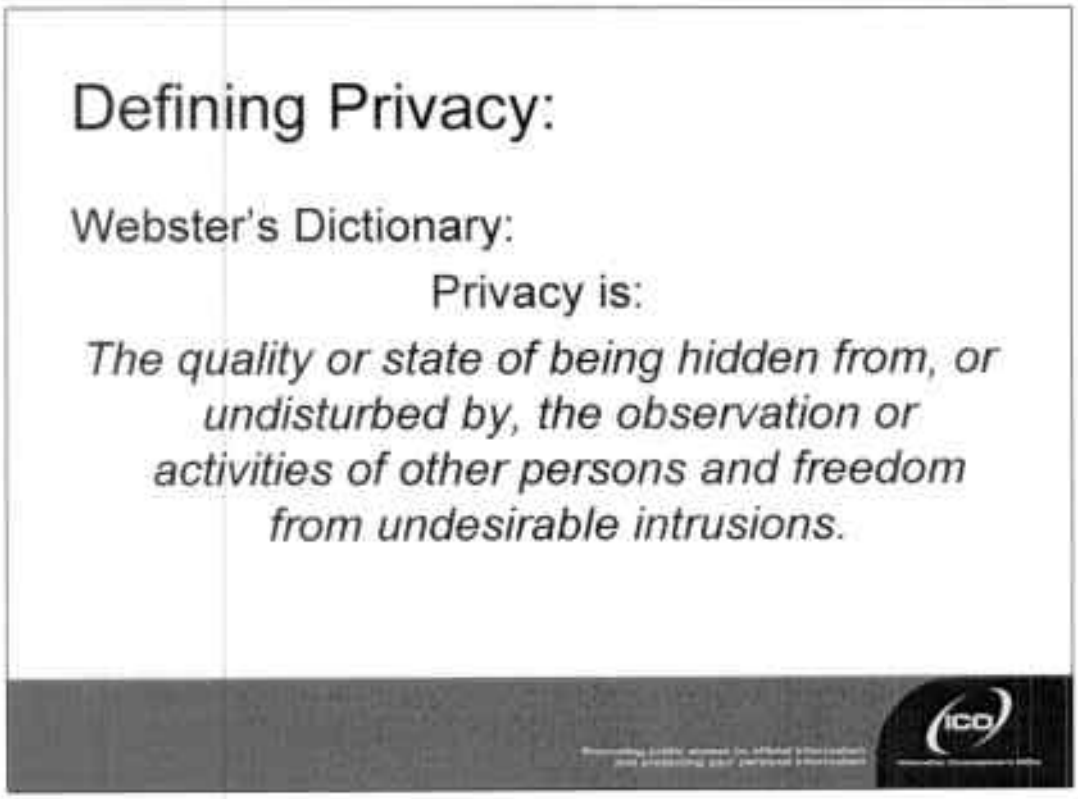
Why Privacy by Design?

•First step towards bridging current gap in development and adoption of privacy-friendly systems.

•There is a clear need for a new approach which will reduce the risks arising from processing personal information and rebuild public trust and confidence.

•It will help put in place a model that will ensure privacy receives the attention it deserves and is fully integrated into information systems in the future.

•The privacy by design programme will encourage public authorities and private organisations to ensure that privacy and data protection compliance are designed into the policy/project rather than ignoring it or bolting it on as an inadequate afterthought.!!

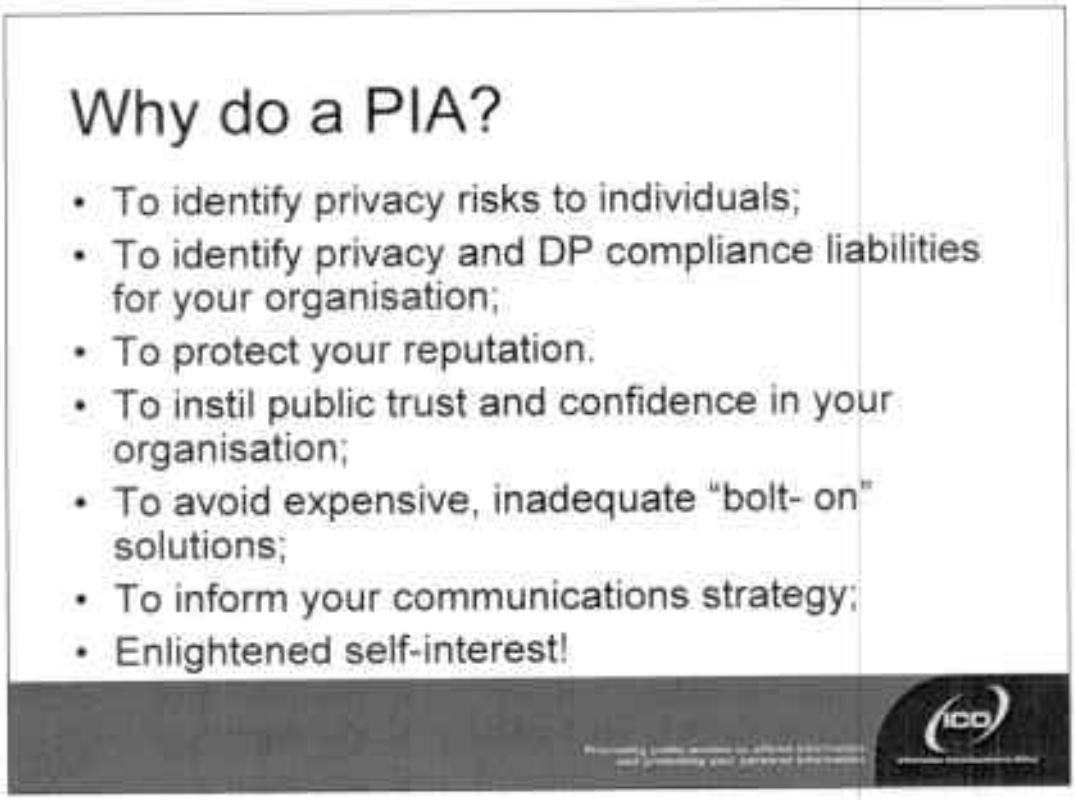


This illustrates the two dimensional nature of privacy –

The right to be undisturbed by the activities of others

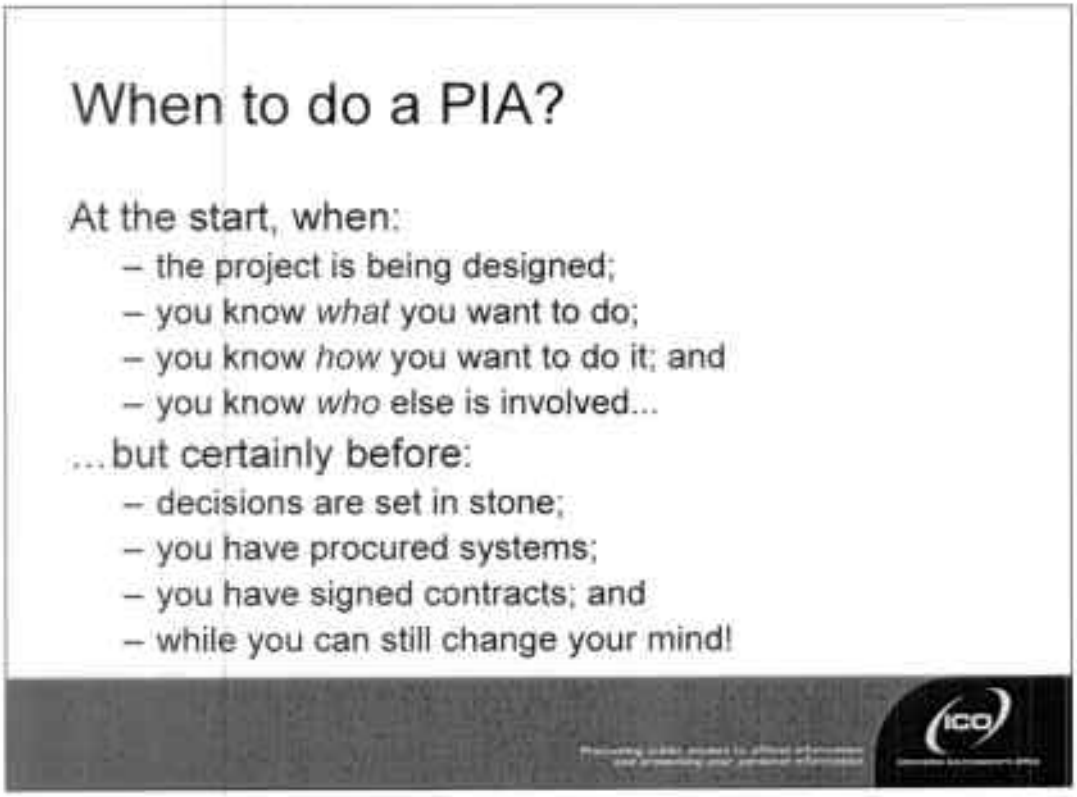
The right to freedom from undesirable intrusions

While at first sight you might question how these two aspect differ as both have the potential for unwanted intrusions on privacy but the former might be viewed as **passive intrusion** - an unintended consequence of another's actions - while the latter is **active intrusion** - the deliberate action of another to intrude upon privacy.



- Risk to individuals
- Risk to organisation
- Risk to reputation
- Instil trust and confidence
- Avoid unnecessary expense
- Ensure appropriate communications
- Know more about yourself!

PIAs go wider than simply a data protection compliance check and are aimed at looking at all aspects affecting privacy. The approach we are recommending involves a number of elements. The important thing about PIAs is the **process** of undertaking the assessment where the organisation considers the impact on privacy and whether there are more privacy friendly alternatives.

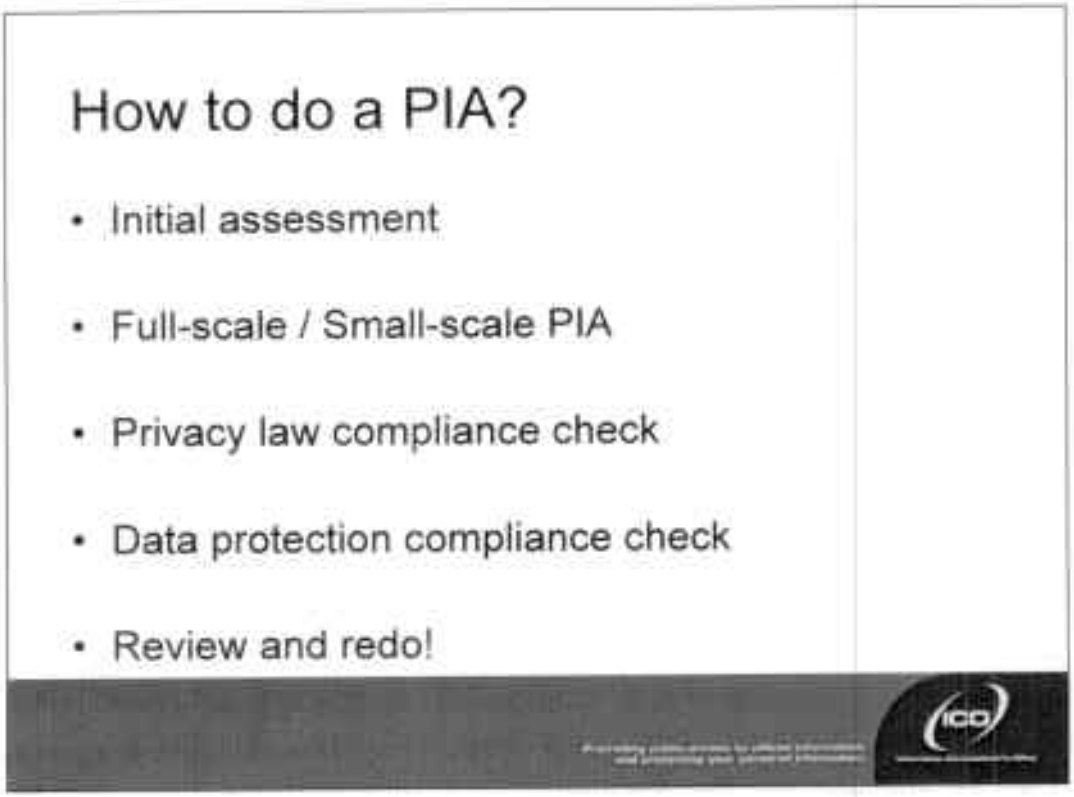


PIAs are a process of ensuring that privacy concerns are identified at the early stage of an initiative so that these can be addressed and safeguards built in rather than bolted on as an expensive afterthought.

Therefore, they are most effective when they are started at an early stage of a project!

Certainly before...

CLICK



•Examines the project at the earliest conceptual stage, makes an initial assessment of privacy risk. Establishes a project team of relevant people. Make sure documentation is up-to-date! Know the technology! 11 Screening questions to determine level of assessment necessary.

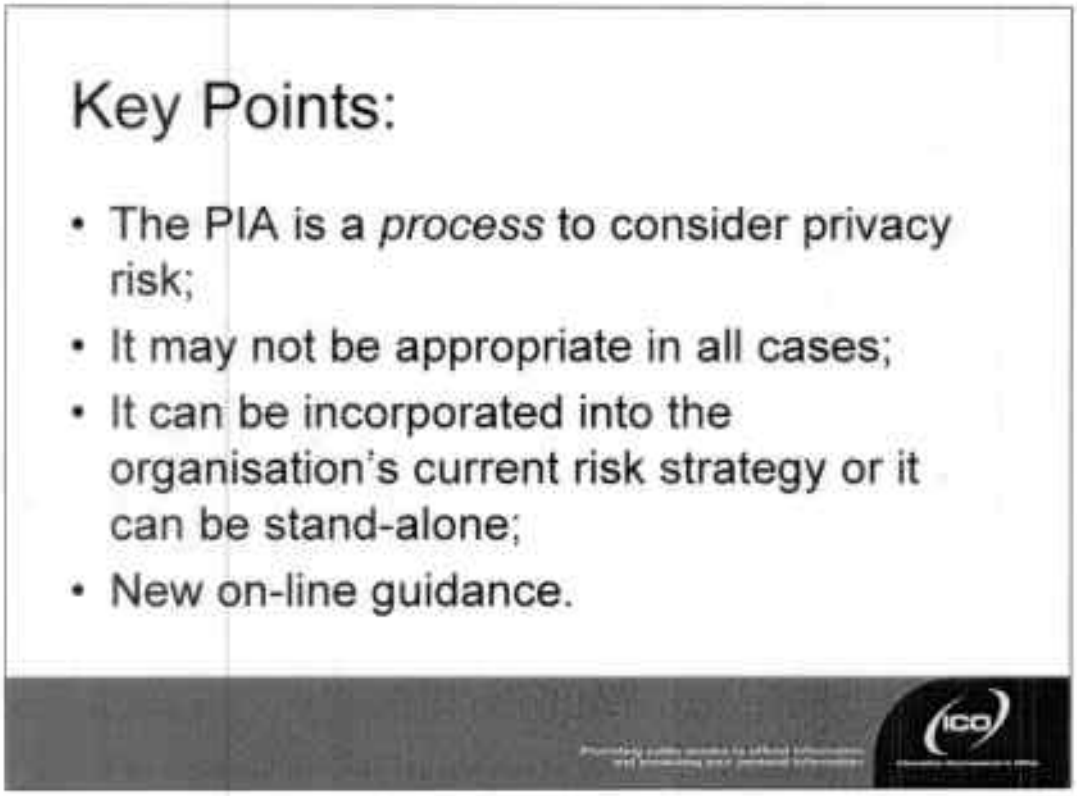
•5 Phases: Preliminary work; Preparation; Consultation/analysis; Conclusions; Review

- **FS**: Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.
- **SS**: Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project.

•Focuses on compliance with various "privacy" laws such as HRA, Regulation of Investigatory Powers Act and PECR. Examines compliance with statutory powers (vires), duties and prohibitions in relation to use and disclosure of personal information.

•Checklist for compliance with DPA. Usually completed when the project is more fully formed.

•Sets out a timetable for reviewing actions taken and examines their effectiveness. Looks at new aspects of the project and assesses whether they should be subject to a PIA



WHAT CAN YOU EXPECT FROM AN EFFECTIVE PIA?

•Identification of potential privacy impacts;

•Appreciation of potential impact and understanding of its acceptability from the stakeholder perspective;

•Identification and assessment of less invasive alternatives;

•How to lessen or even avoid negative impacts on privacy;

•Clarify the business need when negative impacts are unavoidable;

•Develop effective communications strategies for internal and external stakeholders.


ICO
Information Commissioner's Office
www.ico.gov.uk

Information Commissioner's Office

The DPA – Red Tape or Good Practice ?

Ken Macdonald
Assistant Commissioner
Information Commissioner's Office

Data Protection: Understanding Responsibilities
13th October 2009

The DPA – red tape or good practice ?

The DPA – red tape or good practice ?

The DPA – red tape or good practice ?


heraldscotland

Wednesday 10 September 2008 The Herald | sundayherald

Front page | News | Sport | Business | Comment | Blogs | Arts & Ents

BREAKING NEWS: New dru_

Wait for it

Published on 30 Nov 2008

As just sound

An Edinburgh shop who provided a home for a friend's cat was barricaded when he asked the friend's vet for the cat's medical history, only to be told that under the Data Protection Act they couldn't pass on to him the cat's medical records.

He said he tried to calm him down by suggesting: "It's perfectly reasonable – the cat may have had a medical procedure that it didn't want anyone to know about."

The DPA – red tape or good practice ?


Telegraph.co.uk

Home News Sport Finance Lifestyle Comment Travel Culture Technology

UK World UK Politics Celebrities Obituaries Weird Earth Science Health News Jobs

Royal Family Religion Road and Rail Defence Law and order Scotland

Marks & Spencer demand 7-year-old boy's permission to deal with mother's complaint

A mother who complained to Marks staff that her seven year old son's Superman playsuit was faulty was told data protection laws meant they could only deal with him

The DPA – red tape or good practice ?

Proceeds lawfully	Lawful and fair processing
Only collects information it needs	Adequate, relevant, not excessive
Holds correct information	Accurate and up to date
Keeps information only as necessary	Kept no longer than is necessary
Respects individual rights	Respects individual rights
Has good security	Kept secure
	Single Purpose
	International Transfers

The DPA – red tape or good practice ?

Fair and Lawful Processing:

- *Satisfy the conditions for processing (eg consent, legal obligation)*
- *Explain why you're collecting the information, what you'll do with it and who you may pass it on to*
- *Use exemptions appropriately (eg, crime, matters of life and death)*


WARNING
ANYTHING RECORDED ON SECURITY CAMERAS MAY BE USED AT ANY VIEWING TIME

The DPA – red tape or good practice ?

Subject Access

- *The right of an individual to access information held about them*
- *Ensure they are who they say they are*
- *Allowed to charge fee (£10 max)*
- *Don't disclose third party information*


SLANE
I AM NOW CUTTING ALL MY RUDE REMARKS ABOUT THE PATIENT FROM HER FILE.

The DPA – red tape or good practice ?

Direct Marketing

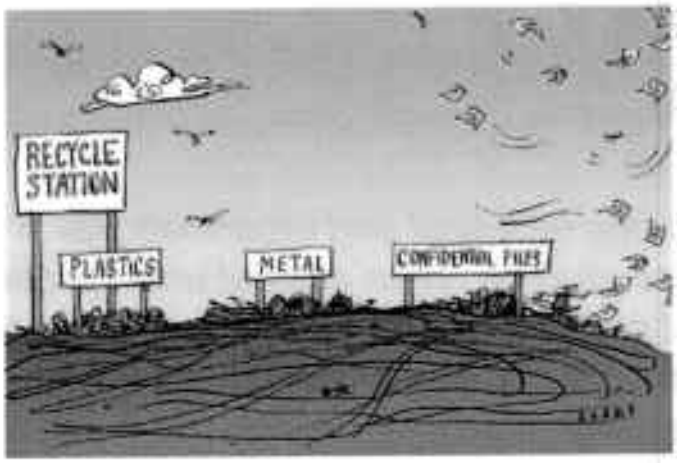
- *The right to stop direct marketing by mail (Data Protection Act)*
- *The right to stop direct marketing by telephone, e-mail & fax (PECR)*


JUNK
THE SOLUTION TO POLITICAL MAIL: THE LETTERBOX/SHREDDER

The DPA – red tape or good practice ?

Security

- *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*


RECYCLE STATION
PLASTICS
METAL
CONFIDENTIAL FILES

If it goes wrong……

Breaches and Offences:

- Breaches: Audits,Undertakings and Enforcement Notices (ie, instructions given to correct procedures)

- Offences: may lead to prosecution

If it goes wrong……

Offences:

- *Unlawfully obtaining or disclosing personal data*
- *Selling of personal data*
- *Failure to notify / notify changes*
- *Failure to comply with a Notice from the Commissioner*
- *Wilful or reckless breach of the DP Principles leading to damage or distress*

If it goes wrong……

Data Controller

- *Reputation Risk*
- *Financial Penalty*

If it goes wrong.....

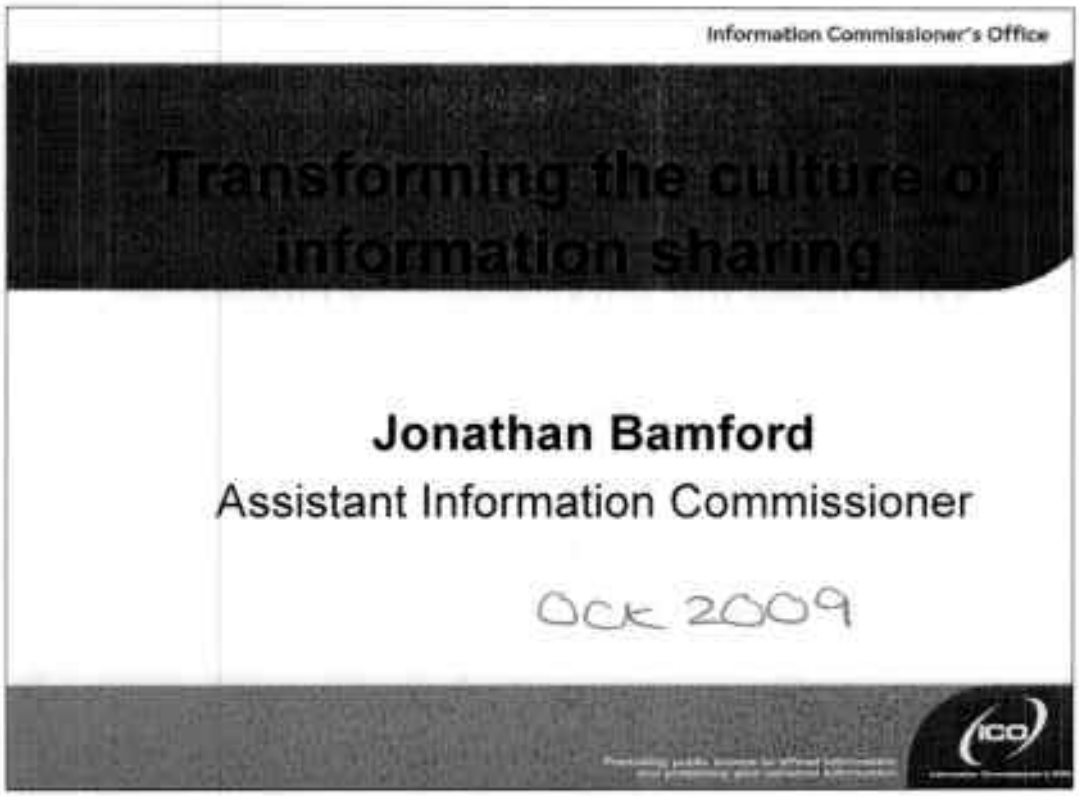
Data Subject

Contact

The Information Commissioner's Office
93-95 Hanover St
EDINBURGH
EH2 1DJ

0131 301 5071
scotland@ico.gsi.gov.uk


ICO
Information Commissioner's Office
www.ico.gov.uk


Information Commissioner's Office
Transforming the culture of information sharing
Jonathan Bamford
Assistant Information Commissioner
OCT 2009

The privacy challenge…

- What does the Information Commissioner do?
- Benefits of information sharing
- Risks for individuals
- Fairness and transparency
- Future developments

The ICO's data protection role.

- "Protecting your personal information"
- Independent regulatory body
- Advice, good practice, enforcement, complaints handling
- 23,000+ complaints / queries and rising.
- Inappropriate data sharing, disclosures, unexpected uses, data breaches...

Data protection =

- Main piece of law regulating personal information
- Records about living, identifiable people
- Right of access
- Standards (security, data quality)
- Necessary, relevant information
- Regulation of disclosure (fair, lawful)
- Transparency

Benefits of information sharing

- Multi-agency co-operation, 'joined-up' services – personalisation
- Convenience – citizens' time is valuable
- Child protection (Contact Point, eCAF)
- Crime reduction partnerships
- Social work / health
- Anti-fraud / anti-terrorism
- New forms of prevention and detection: sophisticated analysis of huge databases

Risks for individuals?

- Do they understand what's happening to information about them?
- How much control do they have over their information? Choice? Consent? Objection?
- Do they understand the consequences of information sharing?
- A growing collection of personal information that more and more officials can access?

Protection for individuals

- Clear purpose for sharing information
- PIA / Privacy by Design
- Periodic review of effectiveness / impact
- Security
- Penalties for abuse of access to databases
- Coroners & Justice Bill: statutory CoP?
- Transparency: explaining information systems
- Framework code of practice for sharing personal information (2007)

Better transparency

- Can be confusing to access shared information
- Law = £10 and wait 40 days
- Cheaper, faster access to records
- On-line access, real-time, free
- Sources and disclosures of information
- Simpler, clearer, more informative 'fair processing notices' (Privacy Notices CoP:2009)

Freedom of Information

- Most information-sharing done by public authorities
- Be prepared to publish your 'paperwork': 'information sharing protocols' etc.
- Public should know when, how and why information about them is being shared
- No blanket exemptions

Future developments

- More intensive use and sharing: but also more targeted / more 'intelligent'
- Blurring of public / private sector
- Stronger penalties for info misuse / crime: board level responsibility
- Better transparency through technology
- PIA / privacy by design
- Better governance

The Personal Information Promise

- A chance to regain public trust and confidence by showing senior level commitment
- Not a regulatory compliance tool
- Opened for signature on European Data Protection Day (28 January 2009)
- PQs applauding those who have signed and questioning others who have not
- Media coverage

I (name and title),
on behalf of (name of organisation)
promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing.

Signed

(name and title)

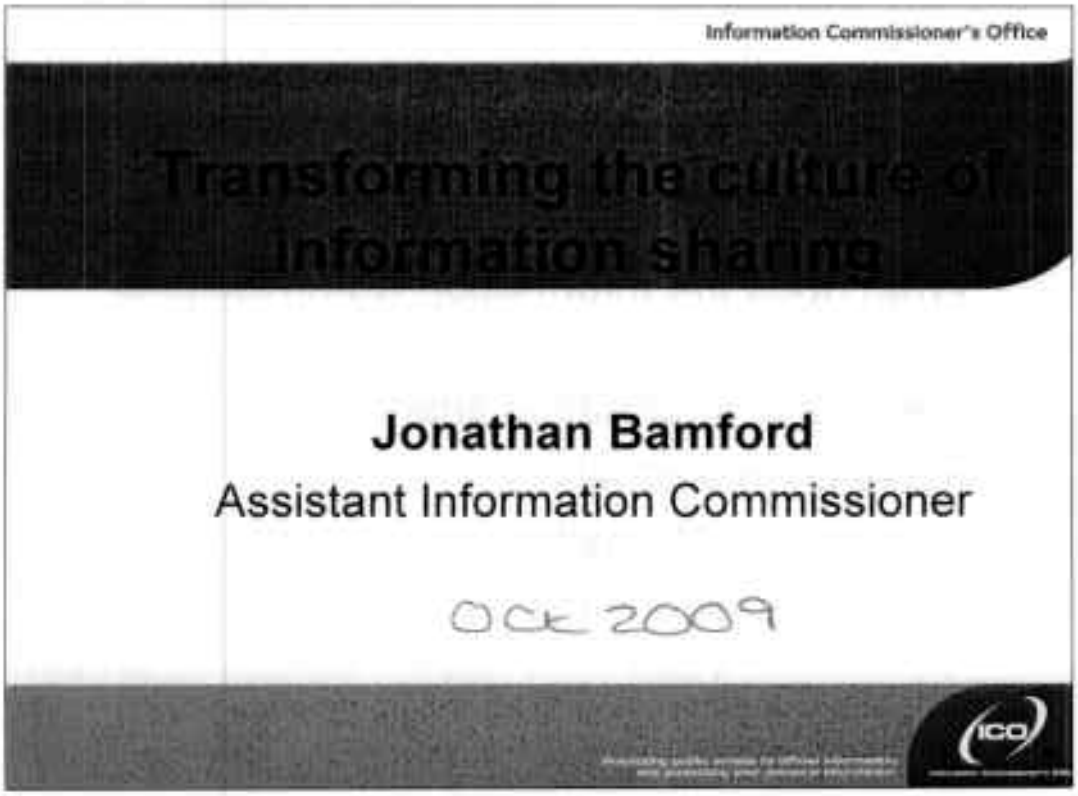
Date

Further Information

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
United Kingdom

Helpline: 08456 30 60 60
E-mail: mail@ico.gsi.gov.uk
www.ico.gov.uk


ICO
Information Commissioner's Office
www.ico.gov.uk


Information Commissioner's Office
Transforming the culture of information sharing
Jonathan Bamford
Assistant Information Commissioner
Oct 2009

The privacy challenge…

- What does the Information Commissioner do?
- Benefits of information sharing
- Risks for individuals
- Fairness and transparency
- Future developments

The ICO's data protection role.

- "Protecting your personal information"
- Independent regulatory body
- Advice, good practice, enforcement, complaints handling
- 23,000+ complaints / queries and rising.
- Inappropriate data sharing, disclosures, unexpected uses, data breaches...

Data protection =

- Main piece of law regulating personal information
- Records about living, identifiable people
- Right of access
- Standards (security, data quality)
- Necessary, relevant information
- Regulation of disclosure (fair, lawful)
- Transparency

Benefits of information sharing

- Multi-agency co-operation, 'joined-up' services – personalisation
- Convenience – citizens' time is valuable
- Child protection (Contact Point, eCAF)
- Crime reduction partnerships
- Social work / health
- Anti-fraud / anti-terrorism
- New forms of prevention and detection: sophisticated analysis of huge databases

Risks for individuals?

- Do they understand what's happening to information about them?
- How much control do they have over their information? Choice? Consent? Objection?
- Do they understand the consequences of information sharing?
- A growing collection of personal information that more and more officials can access?

Protection for individuals

- Clear purpose for sharing information
- PIA / Privacy by Design
- Periodic review of effectiveness / impact
- Security
- Penalties for abuse of access to databases
- Coroners & Justice Bill: statutory CoP?
- Transparency: explaining information systems
- Framework code of practice for sharing personal information (2007)

Better transparency

- Can be confusing to access shared information
- Law = £10 and wait 40 days
- Cheaper, faster access to records
- On-line access, real-time, free
- Sources and disclosures of information
- Simpler, clearer, more informative 'fair processing notices' (Privacy Notices CoP:2009)

Freedom of Information

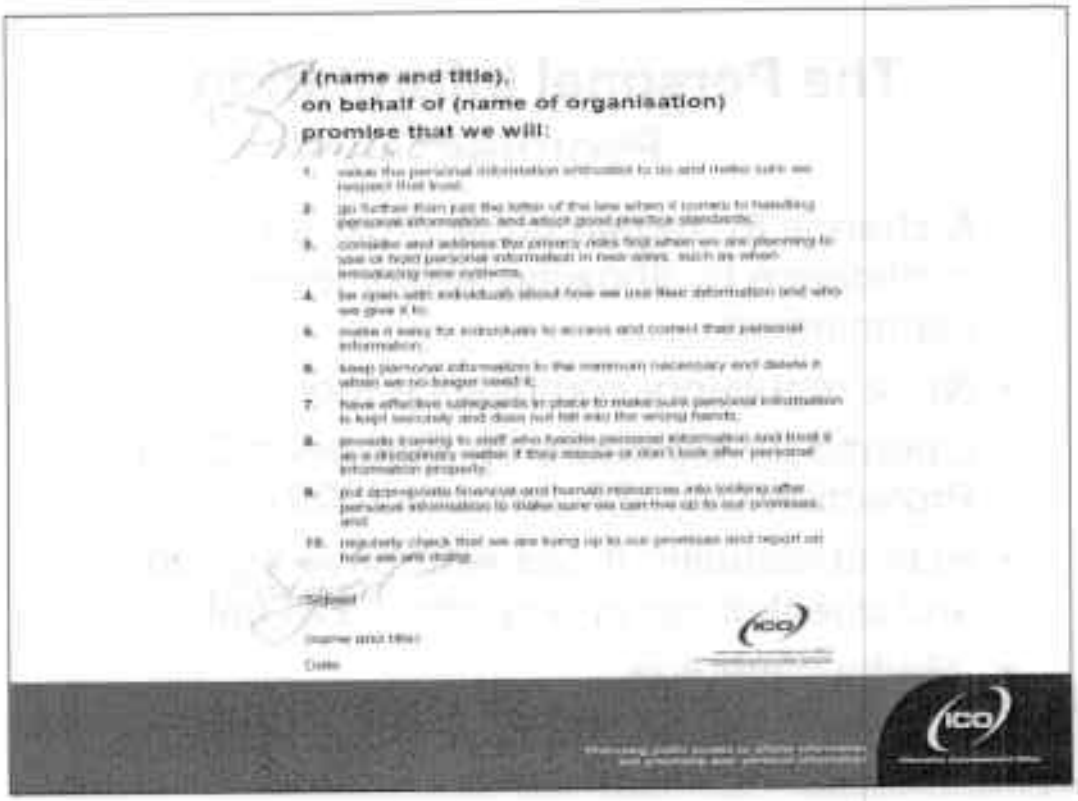
- Most information-sharing done by public authorities
- Be prepared to publish your 'paperwork': 'information sharing protocols' etc.
- Public should know when, how and why information about them is being shared
- No blanket exemptions

Future developments

- More intensive use and sharing: but also more targeted / more 'intelligent'
- Blurring of public / private sector
- Stronger penalties for info misuse / crime: board level responsibility
- Better transparency through technology
- PIA / privacy by design
- Better governance

The Personal Information Promise

- A chance to regain public trust and confidence by showing senior level commitment
- Not a regulatory compliance tool
- Opened for signature on European Data Protection Day (28 January 2009)
- PQs applauding those who have signed and questioning others who have not
- Media coverage



I (name and title),
on behalf of (name of organisation)
promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust.
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards.
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems.
4. be open with individuals about how we use their information and who we give it to.
5. make it easy for individuals to access and correct their personal information.
6. keep personal information to the minimum necessary and delete it when we no longer need it.
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands.
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly.
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises, and
10. regularly check that we are living up to our promises and report on how we are doing.

Signed

(name and title)

Date

ICO

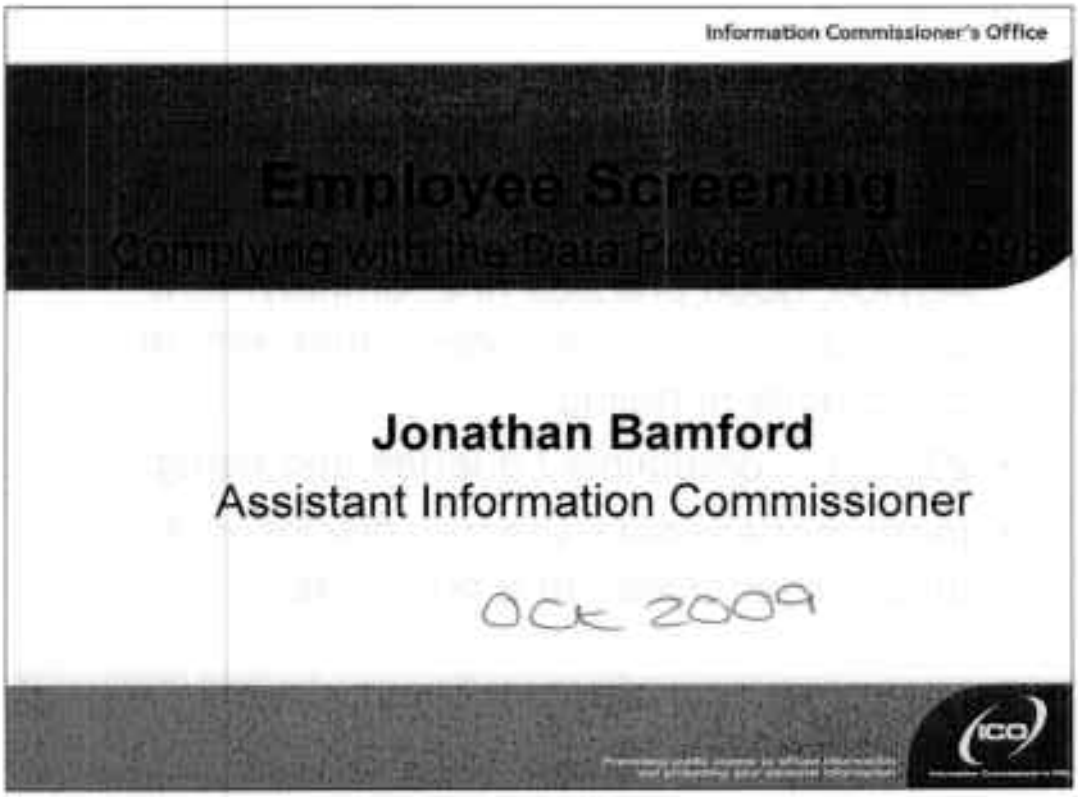
ICO

Further Information

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
United Kingdom

Helpline: 08456 30 60 60
E-mail: mail@ico.gsi.gov.uk
www.ico.gov.uk


ICO
Information Commissioner's Office
www.ico.gov.uk


Information Commissioner's Office
Employee Screening
Jonathan Bamford
Assistant Information Commissioner
Oct 2009

The ICO's data protection role

- Independent regulatory body
- Advice, good practice (inc. employment practices code of practice), enforcement, complaints handling
- 23,000+ complaints / queries and rising.
- Inappropriate data sharing, disclosures, unexpected uses, data breaches...

The Data Protection Principles

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than necessary
- Processed in line with individuals' rights
- Kept secure
- Not transferred to countries without adequate protection

Screening: Key issues

- Is it justified?
  - for all or just some?
- Is there a less intrusive way?
- When is it done?
  - Application, successful applicant, existing workers?
- When are people told?
  - How and what?

Screening: Key issues

- Only use screening to obtaining specific information
  - Clearly stated objectives
  - Focussed on employment decision
- Only seek information from sources likely to be of value
- Do not place reliance on unreliable sources
  - No over reliance
  - Be open if negative
  - Allow individual to respond

Screening: Key issues

- Ensure privacy of third party individuals
  - Avoid discovering unnecessary information
  - Inform third party individuals if details are retained
- If obtaining information or documents from third party get consent
  - Such as information from previous employer
  - Pass this on to third party

Screening: Key issues

- What is recorded?
- Is it used only for that purpose?
- Who is the information shared with?
- Is it held securely?

Screening: Key issues

- In short:
  - Is it justified?
  - Are you open about it?
  - Are the sources reliable?
  - Is the information itself reliable?
  - Is it the minimum information necessary?
  - Can information be challenged by the individual?
  - Is it recorded properly?
  - Used only for a limited purpose?
  - Not disclosed inappropriately?
  - Not retained longer than necessary?
  - Held securely?

Further Information

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
United Kingdom

Helpline: 08456 30 60 60
E-mail: mail@ico.gsi.gov.uk
www.ico.gov.uk


ICO
Information Commissioner's Office
www.ico.gov.uk